English is not an official language of the Swiss Confederation. This translation is provided for information purposes only and has no legal force.

ETH Zurich Acceptable Use Policy for Information and Communications Technology ("BOT") and Appendix

(Partial revision as of 1 May 2022)

RSETHZ 203.21en

English is not an official language of the Swiss Confederation. This translation is provided for information purposes only and has no legal force.

ETH Zurich Acceptable Use Policy for Information and Communications Technology[1]

(BOT)

dated 19 April 2005 (status as of 1 May 2022)

The ETH Zurich Executive Board,

pursuant to Art. 4(1)(c) of the Ordinance Governing the Organisation of ETH Zurich of 16 December 2003[2],

decrees:

1. Section: General provisions

Art. 1 Purpose

[1]The information and communications technology resources (ICT resources) of ETH Zurich should be used in the manner best suited to the pursuit of its mission.

[2]The purpose of this Policy is to ensure the proper use of ETH Zurich ICT resources and their smooth operation.

Art. 2 Definitions[3]

[1]The term "*ICT resources"* comprises all information and telecommunication resources owned by ETH Zurich or used on behalf of ETH Zurich. In particular, it refers to systems, devices and services of ETH Zurich used for electronic data processing (e.g. data processing equipment, network components, data storage devices, printers, scanners, telecommunication networks and related software, locking systems or services outsourced by ETH Zurich, such as cloud solutions). The definition also includes non-ETH-Zurich-owned systems (e.g. private laptops) connected to the data network of ETH Zurich. It does not include video surveillance in accordance with the Swiss Federal Institutes of Technology Act (ETH Act)[4].

[2] The term "*systems*" refers to ICT resources.

[3] The term *"data"* includes personal and academic data.

---

[1] Throughout this Policy, the term "telematics" has been replaced with "information and communications technology" or "ICT". Equally, the term "telematics resources" has also been replaced by the term "information and communications technology resources" or "ICT resources".

[2] RSETHZ 201.021en

[3] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.

[4] Art. 36(i) ETH Act

[4] The term "*users"* includes all members of ETH Zurich (Art. 13 of the ETH Act) and third parties who are authorised to use the ICT resources of ETH Zurich (e.g. guests[5], congress participants, affiliated organisations, library users at public work stations, employees of ETH Zurich's spin-off companies or of other companies, provided a contractual arrangement exists to this effect, professors emeriti and retired employees).

[5] The term "*electronic communication resources*" includes telephone, fax, email, SMS, instant messaging, video conference systems and similar resources.

[6] The term "*organisational units"* refers to the central or decentralised bodies of ETH Zurich established by the Executive Board pursuant to the ETH Zurich Organisation Ordinance (OV) of 16 December 2003[6] (e.g. academic departments, institutes, administrative departments[7], staff units, independent chairs) and the education and research facilities outside the academic departments established pursuant to Art. 61 OV.

[7] The term "*private use*" refers to any use of the ICT or telecommunication resources of ETH Zurich that is not for study purposes, or for the purpose of fulfilling one's duties in the employment relationship.

[8] The term "*analysis of anonymous data*" refers to the statistical analysis of the log files that does not permit the analysis of personally identifiable data.

[9] The term "*analysis of pseudonymous or non-personally identifiable data*" refers to the analysis of the log files of pseudonymised identifiable persons. The pseudonym must protect the identity of the person in question in the phase of monitoring non-personally identifiable data[8].

[10] The term "*logging*" refers to the continuous recording of metadata (addresses in the message headers, session data from the log file in accordance with the technical communication log file and similar data) of the ICT resources.

[11] The terms "*service users*" and "*system and network zone administrators*"[9] refer to the specialists described in the "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich"[10] (IT Guidelines and Basic Security Requirements of ETH Zurich) and in Art. 6 of this decree.

[12] The *Chief Information Security Officer (CISO)* is the person who, in accordance with Art. 5 of the Directive on Information Security at ETH Zurich[11], is responsible for safeguarding IT security across the university. For this purpose, he/she shall work together with the units in accordance with Arts. 6-11 of the Directive on Information Security at ETH Zurich[12].

Art. 3 Scope[13]

This Policy applies to any use of ICT resources by users (for terminology refer to Art. 2(2) and (4)), i.e. it applies to any use or shared use, whether by **ETH Zurich members** or **third parties,** of all ETH Zurich-owned ICT resources and ICT resources used on behalf of ETH Zurich (e.g. outsourced services such as cloud solutions) as well as to any use of non-ETH Zurich devices connected to the ETH Zurich data network.

---

[5] See the Directive of the Vice President for Human Resources and Infrastructure of 13 November 2018 concerning visitor stays at ETH Zurich (RSETHZ 515.2_en).
[6] RSETHZ 201.021
[7] Editorial amendment
[8] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[9] Throughout the decree, the term "network administrator" has been replaced by "network zone administrator".
[10] RSETHZ 203.23
[11] RSETHZ 203.25en
[12] As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
[13] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.

2. Section: Responsibilities

Art. 4 IT Services department, IT support groups and CSCS[14]

[1]The ETH Zurich IT Services department (hereinafter "IT Services") shall provide IT services to the individual users and to the ETH Zurich organisational units. It shall appoint an IT Security Officer for IT Services (ITSO ITS) in accordance with Art. 8 of the Directive on Information Security at ETH Zurich. In particular, IT Services is responsible for the following in the area of IT security (information security section)[15]:

a) The implementation of technical measures with regard to safeguarding IT security for ICT resources and services that are provided by IT Services for the central and decentralised organisational units of ETH Zurich, including the identification and resolution of security defects;

a[bis]) The ETH Zurich-wide technical and operational review of ICT resources[16] for security defects on behalf of the CISO and notification of the persons responsible for resolving them. Reviews of outsourced ICT resources are carried out within the framework of the applicable contractual provisions and testing options that can be reasonably implemented.

a[ter]) Selecting and operating the technical solutions required for these tests, which may be instructed to be carried out in accordance with the requirements of the CISO;

b) Providing training and information for users for the purpose of resolving known security defects;

c) Developing the "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich) and monitoring technical and operational compliance with these on behalf of the CISO for the attention of the Vice President for Infrastructure and the CISO[17];

d) Coordinating the implementation of technical and organisational innovations;

e) Providing the necessary encryption techniques (Art. 13(2)) as per the requirements of the CISO;

f) The duties assigned to it in accordance with the Directive on Information Security at ETH Zurich[18] with regard to information security;

g) Granting exceptions pursuant to Art. 15[bis] with regard to the integrity of the ICT network as per the requirements of the CISO;

h) *revoked*;

i) Exchanging of information within ETH Zurich and the ETH Domain as well as between the universities, SWITCH and the federal authorities, unless this is done by the CISO in accordance with Art. 5 of the Directive on Information Security at ETH Zurich[19];

j) Assisting the CISO[20] in fulfilling his/her tasks pursuant to the Guidelines for Monitoring the Use of ICT Resources at ETH Zurich, attached as Appendix, provided this is not done by other units (e.g. IT support groups or CSCS);

---

[14] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[15] As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
[16] In accordance with the definition in Art. 2 (1), this expressly refers to ICT resources owned and not owned by ETH Zurich.
[17] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021. Please note: the previous documents "IT Best Practice Rules" and "Standards for Responsibilities and System Maintenance" (RSETHZ 203.23) were merged to form a new document "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich) (RSETHZ 203.23).
[18] RSETHZ 203.25en, specifically Art. 10
[19] RSETHZ 203.25en
[20] The term "IT security Officer" has been replaced with "CISO" throughout this document (see Art. 2(12)).

k) *revoked*;

l) Clarifying the admissibility of a commercial use of the ICT resources and concluding the relevant agreements (Art. 8 (6));

m) *revoked*[21].

[2] The IT support groups in the academic departments shall be for the main part responsible for the same tasks within their areas of responsibility, except for the tasks defined under the letters a[bis]), a[ter]), c), i) and g).

[3] In its function as national centre, the Swiss National Supercomputing Centre (CSCS) shall be responsible for providing services in the area of supercomputing, except for the tasks defined under the letters a[bis]), a[ter]), c) and g).

Art. 5 Chief Information Security Officer (CISO)[22]

[1] ETH Zurich has a CISO in order to safeguard information security. He/she has the duties and competencies laid out in Art. 5 of the Directive on Information Security at ETH Zurich[23]. He/she is not affiliated with a specific department and in organisational terms is attached to the President. He/she reports to the Risk Management Commission (RMC) of ETH Zurich.

[2-5] *revoked*

Art. 6 Responsibilities and assessment of security requirements[24]

[1] There is a person responsible for all ICT resources and at least one deputy, specifically a service user for each outsourced ICT service, a system administrator for each ICT resource in the data network of ETH Zurich, and a network zone administrator for each network zone of the data network of ETH Zurich.

[2] Each organisational unit appoints the people responsible for their ICT resources in the data network of ETH Zurich, their network zones, and the outsourced ICT services they use. The associated implementing provisions, incl. the possibilities to delegate duties to service providers (e.g. IT operators), are set out in the "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich).

[2bis] For systems not owned by ETH Zurich that are operated in the data network of ETH Zurich ("bring your own device", BYOD and self-managed systems), the logged-in user is considered by ETH Zurich to be the system administrator if there is no system administrator contactable for the IT Services department.

[3] IT operators of ETH Zurich are as follows: IT Services, CSCS, the academic departments' IT support groups (ISG).[25] Based on the reports from the responsible Information Security Officers (ISO)[26], the IT operators determine which ICT resources process high-risk data within the meaning of Arts. 16 and 23(1) of the Directive on Information Security at ETH Zurich.

[4] The system administrator and the service user have the following duties in particular:

a) They classify the security requirements for systems owned by ETH or outsourced ICT services which are not managed by an IT operator.
b) They are responsible for compliance with and the implementation of the "IT-Richtlinien und IT-

[21] As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
[22] As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
[23] RSETHZ 203.25en
[24] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[25] IT operator in accordance with Art. 3(4) of the Directive on Information Security at ETH Zurich (RSETHZ 203.25en).
[26] Art. 6 Directive on Information Security at ETH Zurich.

Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich)[27].

c) They immediately report security problems, defects etc. to the responsible units in IT Services or the IT support groups.
d) They delete the data of ETH Zurich contained on data storage devices (e.g. hard disks) before they are passed on or disposed of (Appendix to BOT, section 1(7)).

[5] Further duties, competencies and responsibilities of the network zone administrators, system administrators and service users are set out in Art. 17 and Art. 18 as well as the Appendix to the BOT. The "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (Guidelines and Basic Security Requirements of ETH Zurich) also apply[28].

[6] *revoked*

Art. 7 Presence on the intranet/internet[29]

[1] The Corporate Communications administrative department shall be responsible for the presentation of ETH Zurich and of its organisational units on the internet or intranet. It shall issue the corresponding implementation provisions in this regard.[30]

[2] In this context, Corporate Communications must duly comply with the regulations concerning equal treatment of disabled people.[31]

[3] Commercial advertising is prohibited. The President may decide on exceptions. This provision does not apply to the mention of sponsors.

[28] RSETHZ 203.23en
[29] As amended by decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013.
[30] ETH Zurich: Web Policy of 1 September 2016 (RSETHZ 203.22_en) and ETH Zurich Social Media Guidelines of 26 February 2013 (RSETHZ 203.24en).
[31] Disability Discrimination Act of 13 December 2002 (DDA; SR **151.3**); Ordinance on Elimination of Discrimination against People with Disabilities of 19 November 2003 (EPDO; SR **151.31**).

3. Section: Use

Art. 8 Purpose of use and authorisation for use[32]

[1] Use of the ICT resources is permitted for the purposes for which they are made available to the users ("intended use"). This does not apply to applications subject to express authorisation.

[2] Users must restrict their use of the ICT resources to the appropriate extent and to the permitted purposes.

[2bis] The employees of ETH Zurich are responsible for maintaining their email inboxes.[33]

[3-4] *revoked*

[5] Without the written consent of the responsible system administrator, or in the case of outsourced ICT services, without the written consent of the service user, users may not perform any general modifications to the ICT resources provided by ETH Zurich, in particular changes and modifications to software programs. This does not apply to the modifications involved in the proper use of the ICT resources.

[5bis] The deactivation, circumvention or removal of binding security mechanisms require the prior consent of the ITSO IS on behalf of the CISO. The associated implementing provisions are set out in the "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich).

[6] In principle, spin-off companies of ETH Zurich shall use their own ICT resources. Commercial use of ETH Zurich's ICT resources (e.g. pursuant to spin-off agreements) is not in principle permitted. An exception to this is the use of a network connection in a network zone of ETH Zurich. Any costs thereby incurred shall be borne by the respective clients.[34]

[6bis] The operation and use of the supercomputing infrastructure at the CSCS or the use of ICT resources within the framework of a research cooperation shall be contractually agreed upon.

[7] ICT resources owned by ETH Zurich are to be disposed of pursuant to Art. 134 of the Financial Regulations of ETH Zurich[35] as well as Section 8 of the Guidelines for Inventory Management at ETH Zurich[36] of January 2019.

Art. 8bis Private use[37]

[1] Use of ETH Zurich's ICT resources for private purposes, in particular email and internet, is basically permitted, provided it

a. is not excessive,
b. does not conflict or interfere with the user's work or study obligations,
c. does not violate Swiss law (in particular the provisions of the Criminal Code) or rights of third parties (personal rights, copyrights),
d. is not of a commercial nature,
e. and does not damage the reputation of ETH Zurich.

[2] However, it is not recommended that ETH members use ETH Zurich's ICT resources for private purposes because ETH Zurich cannot fully guarantee privacy for private matters. From a technical perspective, private

[32] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[33] As amended by decision of the ETH Zurich Executive Board of 7 April 2022, effective as of 1 May 2022.
[34] As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
[35] Financial Regulations of ETH Zurich of 1 January 2019 (RSETHZ 245en).
[36] Available from ETH Zurich > Finance and Controlling > Downloads (last accessed on 29 June 2021).
[37] As amended by decision of the ETH Zurich Executive Board of 7 April 2022, effective as of 1 May 2022.

emails received or sent via ETH Zurich's ICT resources and private documents that are being worked on are treated as work-related correspondence of ETH Zurich.

[3] Maintenance of personal email inboxes as per Art. 8(2[bis]) includes deleting private emails or moving them to a "Private" folder, where such a folder has been set up by the system administrator, if ETH members wish to avoid these emails being saved on a long-term basis in accordance with para. 4 and later permanently archived. In the email system provided by the IT Services department, such emails must be deleted or moved within 60 days of creation or receipt.

[4] Emails that remain in the ETH member's work inbox in accordance with paragraph 3 are regarded as commercially relevant to ETH Zurich. They are backed up after 60 days at the latest and stored securely and immutably for at least tenyears. After the end of this period, they are offered to the ETH Zurich archives for permanent archiving in accordance with the Federal Act on Archiving[38] and Art. 4 of the Reglement für das Archiv der ETH Zürich[39] (ETH Zurich Archiving Regulations). Emails that the ETH Zurich archives consider to be redundant or not of archival value[40] are deleted.

[5] If the ETH member needs to keep his/her work-related emails beyond the 10-year period for work reasons, he/she must apply to the system administrator to have the deletion process suspended.

[6] Furthermore, this private use of ETH Zurich ICT resources should not technically disrupt or impair their use for purposes appropriate to ETH Zurich's statutory missions, or put excessive load or stress on the generally available resources (networks, internet access, storage capacities, etc.).

[7] Private personal contents of ETH members are not allowed on public ETH web pages, except for curriculum vitae, publications etc. of researchers. IT Services can provide centralised systems required to create personal websites.

[8] Software licenced to ETH Zurich may be used professionally at home ("home office use") by ETH Zurich employees employed on an at least 50% basis, and by the students matriculated at ETH Zurich if permitted by the applicable software licence agreement[41]. The right to install software on a private computer and the type of software use (e.g. right to private use) is governed by the applicable licence agreement. Unless expressly permitted by the licence agreement, parallel use of software licenced to ETH Zurich on a private and office computer is forbidden.[42]

Art. 9 Use of ICT resources outside the ETH Zurich campus[43]

[1] Employees working at home with the consent of the appropriate authority are to use the ICT resources of ETH Zurich accordingly[44].

[2] The use of portable ETH-owned devices, such as laptops, smartphones, etc., is permitted outside of the ETH Zurich campus. The "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich) must be complied with.

---

[38] SR **152.1**
[39] RSETHZ 420.1
[40] According to the assessment decision by the ETH Zurich archives of 31 August 2021, emails of the Executive Board members and the Secretary General are considered to be of archival value, as are documents that are of particular legal or administrative significance or of high informational value.
[41] Explanatory information from IT Services available from https://www.softwareinfo.ethz.ch/home-use-of-eth-software/, last accessed on 29 June 2021. The respective licensing conditions apply.
[42] As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
[43] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[44] Pursuant to Art. 43 of the Personnel Ordinance for the ETH Domain. The employer shall provide employees with the relevant ICT resources required to carry out their work.

Art. 10 Private use of software licenced to ETH Zurich[45]

revoked

Art. 11 Data protection[46]

[1] The processing of personal data[47] is permitted only for the purposes of the pursuit of ETH Zurich's statutory missions in compliance with the data protection regulations.[48]

[2] The disclosure of users' personal data to third parties for authorisation and authentication of electronic services (specifically cloud services) is permitted, provided, however, that this data is not sensitive[49] and is required for the use of the services.

[3] Mass mailings to ETH internal addressees **outside of** one's own organisational unit for information purposes shall be carried out upon written request by the Rectorate or IT Services (on behalf of Corporate Communications/HR). Mass mailings may be initiated upon request by the Executive Board or for interdepartmental announcements of courses, etc. (e.g. course information of D-INFK/D-MATH, training instructions of SSHE).

[4] When using web analysis tools (e.g. Google Analytics), the guidelines of the Swiss Federal Data Protection and Information Commissioner (FDPIC) must be complied with[50].

[5] Any question concerning data protection in general should be directed to the Legal Office.

Art. 12 Software copies[51]

revoked

Art. 13 Use of electronic communication resources[52]

[1] The confidentiality of messages transmitted through ICT resources cannot be guaranteed.

[2] Professional, official and business secrets and other confidential information[53] (e.g. files of staff) may only be transmitted out of the ETH Zurich domain using secure ICT resources, in particular using appropriate encryption techniques, where available.

---

[45] As amended by decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013.
[46] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[47] According to the legal definition of the Federal Act on Data Protection of 19 June 1992 (SR **235.1**), personal data includes all data which refers to a certain or determinable natural or legal person.
[48] Federal Act on Data Protection of 19 June 1992 (DSG; SR **235.1**); Ordinance to the Federal Act on Data Protection of 14 June 1993 (VDSG; SR **235.11**); Art. 59 et seq. of Personnel Ordinance (PVO-ETH; SR **172.230.113**). Also applicable are Art. 36(a) to 36(e) of the ETH Act (SR **414.110**), the "Verordnung über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen" (Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation); SR **172.010.442**) and the "Richtlinien über den Schutz und den Umgang von Personaldaten der ETH Zürich" (Guidelines on protecting and processing personal data at ETH Zurich) (RSETHZ 612).
[49] Data within the meaning of Art. 3(c) of the Federal Act on Data Protection (SR **235.1**).
[50] www.edoeb.admin.ch. Any questions should be directed to the Legal Office or Corporate Communications.
[51] As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
[52] As amended by decision of the ETH Zurich Executive Board of [EB-date NEW], effective as of 1 June 2021.
[53] See Art. 16 and 23 (1)^{bis} of the Directive on Information Security at ETH Zurich (RSETZH 203.25); wording in accordance with decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.

[3] The ICT resources may not be used anonymously, or with a pseudonym, or a false sender.

4. Section: Security measures

Art. 14 Low-risk systems[54]

[1] **Low-risk** systems are systems containing data in accordance with Art. 23(2) of the Directive on Information Security at ETH Zurich for which the basic measures in accordance with Art. 19(1) of the Directive on Information Security at ETH Zurich are sufficient.

[2] *revoked*[55]

[3] *revoked*

[54] As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
[55] Moved to Art. 6

Art. 14bis Access protection measures[56]

[1] Users shall be responsible for the confidentiality of personal access data and identification mechanisms, such as passwords, PINs, private keys, chip cards, physical keys, tokens, etc. They may not disclose or make available this information to third parties, in particular other users.

[2] In the event of suspicion that identification mechanisms[57] or access data of ETH Zurich has been disclosed or made available to unauthorised parties, or has been used by such parties, the user must promptly have his/her access blocked and report the incident to the responsible IT support.

[3] The competent offices of ETH Zurich never request the user to disclose his/her access data by electronic means. If a user is requested to do so, it is an attempt to obtain confidential information for malicious intent (phishing). Such an incident must be promptly reported to the Service Desk of IT Services.

[4] *revoked*

Art. 15 High-risk systems[58]

[1] **High-risk** systems contain data in accordance with Art. 16 and 23(1)^{bis} of the Directive on Information Security at ETH Zurich.

[1bis] *revoked*

[2]Such systems must be more rigorously protected from being accessed by unauthorised third parties in accordance with Art. 19(2) and (3) of the Directive on Information Security at ETH Zurich.

[3] *revoked[59]*

[4-9] *revoked*

[10] The loss or unintended disclosure of ETH Zurich data related to administration, education and research within the meaning of Art. 15(1) must be prevented. Thus, it is incumbent upon each user to ensure that the mobile data storage devices that he/she uses (CDs/DVDs, USB sticks, storage cards, flash storage devices, etc.) and the data on mobile devices are deleted in an appropriate manner und made unreadable before disposal[60]. In case of data loss, the employee's supervisor and the CISO are to be informed. In the event of theft, the SSHE administrative department must also be notified.

[56] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[57] Also means of authentication.
[58] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[59] Updated and moved to Art. 6.
[60] See also Appendix to BOT 1(7).

Art. 15bis Integrity of ICT network[61]

The ICT network of ETH Zurich may not be expanded or modified by users or third parties in an unauthorised manner[62]. Exceptions to this require written consent from IT Services.

5. Section: Responsibility and liability

Art. 16 Responsibility[63]

[1] Every user shall be personally responsible for ensuring that her/his use of the ICT resources does not violate the provisions of this Acceptable Use Policy or of the applicable laws (e.g. criminal law, data protection regulations), or infringe third-party rights (e.g. copyrights, licence terms, personal rights).

[2] *revoked*

Art. 17 Liability

[1] Users are expected to use the ICT resources provided by ETH Zurich with all due care.

[2] The technical and operating instructions issued by IT Services, IT support groups, the CSCS, system administrator, service users, the instructions issued by the CISO as well as the implementing provisions of the BOT and the "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich)*[64]* apply to all users[65].

[3] Unless the responsible bodies have given a guarantee in writing, ETH Zurich shall not be liable for any defects in the ICT resources and their consequences.

[4] In all cases, the user shall be liable for damages or technical disruptions in the ICT resources of ETH Zurich caused by his/her gross negligence or wilful misconduct. In case of non-intended use, the user concerned shall be liable also for minor negligence.

[5] In case of grossly negligent or intentional infringement of third-party rights (in particular copyrights and licence terms), the user shall also be liable for any claims eventually brought against ETH Zurich by third parties.

[6] In other respects, the Government Liability Act applies to the employees of ETH Zurich who use the ICT resources to carry out the Federation's public tasks.[66]

---

[61] As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
[62] E.g. through a connection to a third-party ICT network via a direct connection (e.g. to the internet) or by installing routers, switches, access point, firewalls, load balancers etc.
[63] As amended by decision of the ETH Zurich Executive Board of 17 September 2013, effective as of 1 October 2013.
[64] RSETHZ 203.23 (specifically Art. 8).
[65] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[66] SR **170.32** (Government Liability Act).

6. Section: Abuse and addressing vulnerabilities

Art. 18 Technical and operational system monitoring to detect abuses[67]

[1] On an ongoing basis or on request, the ICT resources shall maintain log files of the most important activities they are used to perform.

[2] Upon instruction by the CISO, non-personally identifiable data contained in the log files may be viewed for spot checks to monitor compliance with the provisions of this Acceptable Use Policy.

[2bis]The log file of emails contains the subject line, date, time, sender and recipient addresses, etc.

[2ter] Data concerning the technical condition of ICT resources, in particular their security status, is collected and analysed by the IT-Security Center of the IT Services department on behalf of the CISO on a continual basis or as part of spot checks.

[3] To address detected abuses within the meaning of Art. 19 or suspected abuses, or to analyse and correct technical malfunctions of the ICT resources and to ward off specific threats to this infrastructure, the data contained in the log files may be analysed on behalf of the CISO with a view to personal references, in accordance with the Appendix to the "Regeln zur Überwachung der Nutzung von IKT-Mitteln an der ETH Zürich" (Guidelines for Monitoring the Use of ICT Resources at ETH Zurich).

[3bis] The Head of the Safety, Security, Health and Environment administrative department is responsible for determining (data recording, sighting, securing) and potentially sanctioning (themselves or via criminal complaint) any abuses, security breaches or crimes via video recordings or electronic access control for buildings or sites of ETH Zurich. The provisions of this Section 6 of the BOT as well as the Appendix shall apply analogously unless any other standards take precedence.

[4] Detailed provisions concerning the determination of the system status, records of user behaviour, responsibilities, recording of abuses, storage of usage data and their analysis are set forth in the Appendix ("Regeln zur Überwachung der Nutzung von IKT-Mitteln an der ETH Zürich" – Guidelines for Monitoring the Use of ICT Resources at ETH Zurich*)*.

[5] The users, service users, system administrators, network zone administrators and IT operators are obliged to assist in investigating the cases of abusive and illegal use, and of any loss or damage.

Art. 19 Abuses

[1] Any use of the ICT resources of ETH Zurich which disregards the provisions of this Acceptable Use Policy, or breaches applicable superordinate laws or infringes third-party rights constitutes an abuse.

[2] In particular, abuses include the following and are forbidden:

a) Processing, storing or transmitting illegal or immoral materials, such as violent images, pornography (Art. 197 of the Swiss Criminal Code "SCC" [SCC; SR 311.0]), incitement to crime or violence (Art. 259 SCC), violations of the freedom of faith and worship (Art. 261 SCC) or racial discrimination (Art 261bis SCC).

b) Writing, providing instruction in writing or intentionally distributing destructive programs or program parts within the meaning of Art. 144bis(2) SCC (viruses, worms, trojan horses, etc.). Providing instruction in writing such programs for teaching and research purposes may be permitted, provided

[67] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.

appropriate measures against malicious use are taken, and subject to the prior written consent of the ETH Executive Board or of its designee.

c) Unauthorised access to a computer system (Art. 143bis SCC, "Hacking"): Cracking passwords, scanning internal and external networks without authorisation in order to identify vulnerabilities (e.g. port scanning), conceiving and executing strategies to disrupt networks and computers (e. g. denial of service attacks). In particular cases, hacking may be permitted in a secure test environment for teaching and research purposes[68], subject to the prior written consent of the ETH Executive Board or its designee; the responsible network zone administrators, system administrators and the ITS IT-Security Center[69] may scan a restricted area for vulnerabilities in order to eliminate them.

d) Data theft (Art. 145 SCC) and data damage (Art. 144bis(1) SCC);

e) Using the ICT resources of ETH Zurich in intentional breach of licence terms and copyrights;

f) Transmitting messages via electronic communication means with forged or misleading sender information or content (e.g. fraudulent e-mails such as phishing, CEO fraud);

g) Harassing or misleading members of ETH Zurich or third parties through messages transmitted by electronic communication means (e.g. with offensive, sexist, racist, defamatory or discriminatory content);

h) Setting up direct access to ETH Zurich communication networks (e.g. through modems or WLAN access points) without prior written consent of IT Services and the responsible system administrator (Art. 15bis);

i) Sending mass advertising without direct links to requested content and without prior consent of the clients, correct sender information or offer of a possibility to decline without problems and costs (spam); this provision does not apply to ETH internal mass mailings within the meaning of Art. 11(3) of this Acceptable Use Policy.

[3] Serious abuses are deemed to be:

a) abuses pursuant to paragraphs 2a), b), c), d) where deliberate or intentional;

b) or other abuses where repeated.

[4] The immediate supervisor, the ITS IT-Security Center of IT Services, the service users and the system or network zone administrators are obliged to report any serious or repeated abuses to the CISO[70].

Art. 20 Consequences of abuses[71]

[1] Should an abuse within the meaning of Art. 19 of this Acceptable Use Policy be detected or reasonably suspected, the CISO may take the following measures:

a) Issue a warning for minor breaches of this Acceptable Use Policy;[72]

b) Suspend access to the ICT resources[73] affected, as a precaution;

c) Block abusive and illegal data, and store and safeguard them as evidence;

d) Delete abusive and illegal data where this is required for security reasons.

[68] E.g. Information Security Lab, D-INFK.
[69] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021; change of name from "Network Security Group" to "IT-Security Center".
[70] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[71] As amended by decision of the ETH Zurich Executive Board of (NEW EBD date), effective as of 1 June 2021.
[72] As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
[73] See also point 4 of Appendix.

[2] As sanctions against abuses, the violators may have their access to the ICT resources blocked, or their use restricted or prohibited. Sanctions shall be revoked if disciplinary proceedings have not been initiated, or a criminal complaint has not been lodged, within three months.

[3] *revoked*

[4] In addition, disciplinary measures or measures under human resources law[74], civil proceedings (action for damages) or criminal complaints may be initiated or lodged against violators[75]. Particularly serious offences (Art. 19(3)) may result in dematriculation or dismissal.

[5] A serious abuse by students does not constitute a petty offence within the meaning of Art. 8 of the ETH Zurich Disciplinary Code[76]. For employees, any type of abuse shall be deemed a breach of duties under labour law[77].

[6] ETH Zurich may pass on to the violator the costs resulting from the abuses and their consequences, including investigation and imposition of sanctions (including investigation, court costs and attorney fees).

Article 20[bis] Addressing vulnerabilities[78]

[1] In accordance with the "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich), any technical vulnerabilities established in ICT resources must be resolved or mitigated to the extent that they do not present a risk to other ICT resources or to data resources of ETH Zurich.

[2] If technical vulnerabilities in ICT resources are not resolved or sufficiently mitigated by the responsible person within 20 days of their being identified, the IT-Security Center of IT Services is authorised to block access to the ICT resources if the vulnerability is critical and other ICT resources or data resources could be placed at risk by this vulnerability. The IT-Security Center of IT Services shall notify the CISO immediately of such cases.

[3] In the event of urgent, acute threats or attacks involving significant risks to the information security of ETH Zurich which require immediate action to be taken, the IT Security Officer of IT Services (ITSO IS) or the responsible IT operator – on behalf of the CISO – may order that security updates be distributed and installed immediately. The ITSO IS / IT operator shall then immediately notify the CISO of such cases.

[4] Any infringements in addressing vulnerabilities may result in a warning from the CISO. Any intentional infringements may be considered serious abuses within the meaning of Art. 19(3)(b) and result in sanctions.

[74] Students: pursuant to Art. 3 of ETH Zurich Disciplinary Code of 2 November 2004 (SR **414.138.1**);
Employees: pursuant to Art. 58a of Personnel Ordinance for the ETH Domain of 15 March 2001 (SR **172.220.113**).
[75] The procedure is based on Art. 22a Federal Personnel Act (FPA; SR **172.220.1**).
[76] ETH Zurich Disciplinary Code of 4 November 2004 (SR **414.138.1**).
[77] Art. 25 Federal Personnel Act (SR **172.220.1**) / Art. 53 Personnel Ordinance ETH; Wording in accordance with decision of the ETH Zurich Executive Board of 20 August 2013, effective as of 1 October 2013.
[78] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.

7. Section: Special provisions

Art. 21 Special provisions and instructions[79]

[1] In other respects, the users, service users, system administrators and network zone administrators must comply with the following regulations, where they relate to their activity or ICT resources they use, in their current version.

a) Any special instructions issued by the organisational units in question concerning use of individual systems, in particular concerning data protection and data security;

b) Implementing Provisions Concerning the Appearance of ETH Zurich on the Internet[80];

c) Guidance for inventory management at ETH Zurich of January 2019[81];

d) "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich)[82];

e) Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation[83];

f) Art. 36a to Art. 36e of the ETH Act [84] (Personnel Information Systems, Student Information Systems; managing personal data in research projects); and

g) *revoked*[85]

[79] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[80] ETH Zurich: Web Policy of 1 September 2016 (RSETHZ 203.22en) and Social Media Guidelines of ETH Zurich of 26 February 2013 (RSETHZ 203.24en). Footnote updated, effective as of 1 April 2019.
[81] Guidance for inventory management at ETH Zurich of January 2019; available from ETH Zurich > Finance and Controlling > Downloads (last accessed on 29 June 2021).
[82] "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich) (RSETHZ 203.23).
[83] Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation of 22 February 2012 (SR **172.010.442**).
[84] ETH Act (SR **414.110**)

8. Section: Final provisions

Art. 22 Enforcement[86]

revoked

Art. 23 Abrogation of previous regulations and effective date[87]

[1] The following decrees have been revoked:

a) ETH Zurich Acceptable Use Policy for Information and Communications Technology (BOT; RSETHZ 203.21en; as of 1 April 2019);

b) IT Best Practice Rules[88] (as of 3 June 2019) and the Standards for Responsibilities and System Maintenance (as of 6 February 2003; RSETHZ 203.23en).

[2] This decree is effective as of 1 May 2005.

Article 24 Coordination with the Directive on Information Security at ETH Zurich and the "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich)[89]

The following articles of this decree only enter into force together with the entry into force of the impending partial revision of the Directive on Information Security at ETH Zurich (RSETHZ 203.25en) and the "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich) (RSETHZ 203.23)[90]:

Art. 2(11)
Art. 4(1)(c)
Art. 6(2), (4)(b) and (5)
Art. 8(5bis)
Art. 9(2)
Art. 17(2)
Art. 18(5)
Art. 19(4)
Art. 20bis(1)
Art. 21(1)(d)
Art. 23(1)(b)
Sections 2.1, 3.1, 3.3 and 7.1 Appendix to the BOT

[86] As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
[87] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[88] The IT Best Practices Rules were adopted by the IT Services department as a recommendation, but never formally entered into force. For the purpose of clarity, they are listed here as having been revoked. As is the case for the Standards for Responsibilities and System Maintenance (RSETHZ 203.23en), they have been replaced by the "IT-Richtlinien und IT-Grundschutzvorgaben der ETH Zürich" (IT Guidelines and Basic Security Requirements of ETH Zurich), which entered into force separately.
[89] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[90] expected as of 1 July 2021.

Zurich, 19 April 2005

On behalf of the ETH Executive Board:

President:	Kübler
Representative:	Kottusch

Appendix[91]

Guidelines for Monitoring the Use of ICT Resources at ETH Zurich

1. Data collection, storage and deletion

[1] Technical prevention, raising awareness and involvement of members of ETH should be given priority over monitoring. ETH Zurich shall ensure that the protective technical measures are regularly updated to the latest state of the art.

[2] If the ICT resources of ETH Zurich are used or ICT resources are operated on the latter's behalf, any data collected may be recorded for the following purposes[92]:

a. all data, including content of electronic mail: for backup purposes (backups);
b. data on the technical state of the ICT resources (e.g. patch statuses, virus protection notifications, vulnerability scans) and marginal data about their use:
   - to ensure information and service security,
   - to conduct maintenance of the electronic infrastructure,
   - to carry out spot checks for compliance with the BOT,
   - to record access to data collections,
   - to control costs;
c. data on entry and exit to and from buildings and rooms of ETH Zurich and times spent therein: for security purposes.

[3] To the extent required by the purpose of the analysis, data mentioned in para. 2 can be stored at the most as follows:[93]

a. data mentioned in 2(a): until the basic underlying information is permanently filed in the ETH Zurich archives[94]; if it is not included: 2 years
b. data mentioned in 2(b): 2 years
c. data mentioned in 2(c): 3 years

[4] The collected data must be deleted by the competent bodies upon expiration of the storage period.

[5] For electronic mail (email) data that is commercially or legally relevant to ETH Zurich, the statutory storage period of 10 years until archiving or deletion is applicable.[95]

[6] For processing and storage of data stored in the personnel and student information systems of ETH Zurich pursuant to Art. 36(a) and 36(b) of the ETH Act, the relevant implementation provisions of the ETH Board or of the ETH Zurich Executive Board[96] are applicable.

---

[91] As amended by decision of the ETH Zurich Executive Board of 9 April 2018, effective as of 1 April 2019.
[92] Recording for the purposes under Art. 57 of the Ordinance on the Organisation of the Government and the Federal Administration (GAOO; SR **172.010**); editorial amendment, effective as of 1 January 2019.
[93] Art. 4 of the Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation of 22 February 2012 (SR **172.010.442**).
[94] The ETH Library has been given the function of public archives for ETH Zurich and the ETH Board pursuant to the Federal Act on Archiving (ArchA; SR **152.1,** RSETHZ 420.1).
[95] As amended by decision of the ETH Zurich Executive Board of 7 April 2022, effective as of 1 May 2022.
[96] "Richtlinien über den Schutz und den Umgang mit Personaldaten an der ETH Zürich" (Guidelines for the Protection and Use of Personal Data at ETH Zurich) of 15 November 2011 (RSETHZ 612).

[7] The storage period and deletion of data on printers, scanners, etc., depend on the storage capacity of the device on which they are stored. This data must be deleted irrecoverably at the latest at the time of transfer or disposal of the device[97].

[8] For the storage of research data, Art. 11 of the Guidelines for Research Integrity and Good Scientific Practice at the ETH Zurich is applicable.[98]

2. Responsibilities

2.1 IT operators, system administrators and service users of the organisational units

a) To install and operate the ICT resources allowing the recording of data pursuant to Section 1 of this Appendix.

b) To carry out spot checks pursuant to Section 3 as instructed by the CISO.

c) To support the CISO and/or ITSO ITS in fulfilling his/her tasks pursuant to these Guidelines.

2.2 Network zone administrators

To support the IT security officer in fulfilling his/her tasks pursuant to these Guidelines.

2.3 IT Services of ETH Zurich:

a) To support the CISO in fulfilling his/her tasks pursuant to these Guidelines and to monitor the ICT resources (i.e. ICT network) of ETH Zurich.
b) Recording of the technical statuses of the ICT resources in accordance with Art.18 (2ter) and Art. 20bis(2).[99]

2.4 IT Security Officer of IT Services (ITSO ITS)

Unless otherwise regulated in Art. 8 of the Directive on Information Security at ETH Zurich[100], the ITSO ITS is specifically responsible for mandating the random checks on behalf of the CISO pursuant to Section 3(1) of this Appendix.

2.5 Chief Information Security Officer (CISO)

Unless otherwise regulated in Art. 5 of the Directive on Information Security at ETH Zurich[101], the CISO is specifically responsible for the following duties:

a) Contacting the Post and Telecommunications Surveillance Service (PTSS);

b) Instructing that spot checks be carried out in accordance with Section 3(1) of this Appendix;

c) Taking preventive measures in accordance with Section 4 of this Appendix;

d) Deciding on the analysis of personally identifiable data in accordance with Section 5(1a) of this Appendix[102];

e) Questioning members of ETH Zurich in accordance with Section 3(2) of this Appendix;

f) Ordering the recording of personally identifiable data in consultation with the responsible direct

[97] Art. 5 of the Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation of 22 February 2012 (SR **172.010.442**).
[98] Guidelines for Research Integrity and Good Scientific Practice at ETH Zurich of 14 November 2007 (RSETHZ 414en).
[99] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[100] Directive on Information Security at ETH Zurich of 9 April 2018 (RSETHZ 203.25en).
[101] Directive on Information Security at ETH Zurich of 9 April 2018 (RSETHZ 203.25en).
[102] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.

line manager (for employees) / the Director of Studies (for students) in accordance with Section 5.

2bis Analysis of recorded log files[103]

The analysis of the recorded log files can concern both non-personally identifiable data and personally identifiable data and must comply with the principles laid down in these Guidelines.

3. Spot checks of non-personally identifiable data[104]

[1] On instruction by the CISO, the system administrators and service users may carry out spot checks of non-personally identifiable data to monitor the use of the ICT resources.

[1bis] For the purpose of monitoring ICT security, the analysis of data not connected to individuals by name (anonymously or pseudonymously) can be carried out by IT Services at any time and without the CISO's instruction in accordance with Art. 1(2) (b)[105].

[2] When monitoring email traffic, the content of private emails of ETH members may not be accessed (Art. 18 (2bis). If an email is not saved in a "Private" folder in accordance with Art. 8bis(3)[106], if the private and work-related emails are not marked as such, and if the address elements give no clue or indication as to the nature of certain messages, ETH Zurich may assume that the email is work-related. In case of doubt, the issue is to be clarified with the ETH member in question.

[3] The abuses actually detected or reasonably suspected in such spot checks must be promptly reported by the system administrators and service users to the CISO.

4. Protective and precautionary measures

[1] If spot checks of non-personally identifiable data give rise to a reasonable suspicion that an abuse within the meaning of Art. 19 BOT has taken place which threatens to jeopardise substantially the use of ETH Zurich ICT resources, or cause damage to ETH Zurich, or to its members, or to third parties, the CISO shall be authorised to take the following protective and precautionary measures[107]:

a) To block access to the ICT resources in which the detected abuse occurs or which are affected by it;

b) To block the data, and store and safeguard them as evidence.

[2] In emergency cases, the ITSO ITS may also request that the measures set forth in para. 1 be taken; the CISO must be promptly notified and shall decide whether the measures taken should remain in effect.

5. Analysis of personally identifiable data[108]

[1] If the analysis of non-personally identifiable data reveals abuses within the meaning of Art. 19 BOT, or gives rise to a reasonable suspicion of such abuses, the CISO may direct that recorded personally identifiable data be analysed according to the following principles:

a) Depending on the seriousness of the abuse, together with the immediate line manager and the Head of HR (employees) or the relevant personnel manager, or with the Director of Studies or the Rector (students), he/she may decide whether the personally identifiable data is to be analysed at once to

[103] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[104] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[105] Editorial amendment of 15 July 2019 (replacement of "Article" with "Section" [of this Appendix]).
[106] As amended by decision of the ETH Zurich Executive Board of 7 April 2022, effective as of 1 May 2022.
[107] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.
[108] As amended by decision of the ETH Zurich Executive Board of 11 May 2021, effective as of 1 June 2021.

identify the violator, or only when the abuse is repeated.

b) In any case, further analyses may be carried out only after the person concerned has been informed about the suspected abuse[109].

c) If the suspected abuse could reasonably constitute a **criminal offence** pursuant to the Swiss Criminal Code, the relevant evidence consisting of log files and, if any, backups, must be secured. **In such cases, follow-up investigations of personally identifiable data are not permitted, and are the sole responsibility of the competent criminal prosecution authorities.** If the guilty parties are ETH teaching staff or employees, the decision whether to lodge a complaint rests with the President[110].

d) *revoked*

[2] Investigations conducted to detect and correct *technical malfunctions* in the ICT resources and to address concrete threats to that infrastructure are permitted only where they are indispensable to search for the cause of the malfunction, or to remedy it, or to ward off a real threat, namely when:

a) the use of the ICT resources has been precluded or substantially impaired by a defect or excessive use by a single user; or

b) there exists a direct risk of damage to the ICT resources, or to the data of the users (spread of malware).[111]

6. Sanctions

The responsibility for imposing sanctions for abuses is governed by Art. 20 BOT.

7. Confidentiality

[1] The data collected pursuant to Section 1 of this Appendix must be treated in confidence; the system administrators and service users must take the appropriate measures to prevent members of ETH Zurich and third parties from gaining unauthorised access to, or knowledge of, such confidential information.

[2] The results of the spot checks and of the analysis of personally identifiable data as well as the protective and precautionary measures must be kept in strict confidence by the persons involved. Information may be disclosed only when and to the extent that the disclosure is permitted pursuant to the present and future applicable provisions.

8. Monitoring of the telephone network

[1] The CISO is responsible for contacting the Post and Telecommunications Surveillance Service (PTSS) operated by the Federation. The PTSS evaluates post and telecommunications for the purpose of investigating serious crimes. The CISO and the other units of ETH Zurich shall also promptly inform the Legal Office if they are contacted by the PTSS, or by the criminal prosecution authorities in relation to the monitoring of the telephone network.

[109] Art. 57o (1)(a) of the Ordinance on the Organisation of the Government and the Federal Administration (GAOO; SR **172.010**) in conj. with Art. 11 of the Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation of 22 February 2012 (SR **172.010.442**).
[110] Art. 14(2) of the "Geschäftsordnung der Schulleitung" (Procedural Rules of the ETH Executive Board) of 10 August 2004 (RSETHZ 202.3).
[111] Art. 57o (1)(b) of the Ordinance on the Organisation of the Government and the Federal Administration (GAOO; SR **172.010**) in conj. with Art. 12 of the Regulation on the Processing of Personal Data Collected through the Use of the Electronic Infrastructure of the Federation of 22 February 2012 (SR **172.010.442**).

[2] Monitoring shall specifically be conducted pursuant to Arts. 4(18) et seq., 28 and 51 et seq. of the "Verordnung über die Überwachung des Post- und Fernmeldeverkehrs" (Ordinance on the Surveillance of Post and Telecommunications) of 15 November 2017 (VÜPF; SR **780.11**).